Post-Quantum Fully Homomorphic Encryption with Group Ring Homomorphisms

Maya Gusak and Chris Leonardi

ISARA Corporation

Abstract

Gentry's groundbreaking work [8] showed that a fully homomorphic, provably secure scheme is possible via bootstrapping a somewhat homomorphic scheme. However, a major drawback of bootstrapping is its high computational cost. One alternative is to use a different metric for noise so that homomorphic operations do not accumulate noise, eliminating the need for boostrapping altogether. Leonardi and Ruiz-Lopez present a group-theoretic framework for such a "noise non-accumulating" multiplicative homomorphic scheme [12], but Agathocleous et al. expose weaknesses in this framework when working over finite abelian groups [1]. Tangentially, Li and Wang present a "noise non-accumulating" fully homomorphic scheme by performing Ostrovsky and Skeith's transform [18] on a multiplicative homomorphic scheme of non-abelian group rings [14]. Unfortunately, the security of Li and Wang's scheme relies on the Factoring Large Numbers assumption, which is false given an adversary with a quantum computer [22]. In this work, we seek to modify Li and Wang's scheme to be post-quantum secure by fitting it into the Leonardi and Ruiz-Lopez framework for non-abelian rings. We discuss improved security assumptions for Li and Wang encryption and assess the shortcomings of working in a non-abelian setting. Finally, we show that a large class of semisimple rings is incompatible with the Leonardi and Ruiz-Lopez framework.

1 Introduction

Fully homomorphic encryption has often been referred to as the "holy grail" of cryptography after it was proposed by Rivest, Adleman and Dertouzos in 1978. Since then, a working fully homomorphic scheme was discovered by Gentry in 2009 [8]. Gentry's scheme is based on the *learning with errors* (LWE) problem on lattices, which can be thought of as finding solutions to a system of noisy linear equations. Due to worst-case to average-case reductions of LWE, it is a promising security assumption [21]. However, homomorphic operations on noisy equations compound noise, making decryption errors more likely. The first ingredient in Gentry's scheme is a bounded-depth homomorphic encryption scheme with security based on the hardness of LWE. The second ingredient is a bootstrapping algorithm which periodically reduces the accumulated noise in ciphertexts, making it then theoretically possible to perform an unbounded

number of homomorphic operations. For a somewhat homomorphic scheme to be bootstrappable, it needs to satisfy an additional *circular security* assumption, which requires semantic security even if an encryption of the secret key under the public key is made public. Gentry's original scheme proved that fully homomorphic encryption is possible, but it was too inefficient to be practical. Since then, a number of improvements have been made [4][9][7][3][6][11].

It is natural to interpret homomorphic encryption through the framework of groups, and in fact there are many examples of group-based encryption which initially seemed to lend themselves nicely to homorphic encryption (see textbook RSA, ElGamal, Goldwasser-Micali, and [25] for more examples). However, the work of Armknecht et. al [2] showed that IND-CPA security is not possible for abelian groups when attacked by a quantum enabled adversary.

Leonardi and Ruiz-Lopez propose abstracting the notion of "learning", "noise", and "rounding" and study a generalized version of LWE in a generic group setting [12]. LWE is based on erasing an error by rounding to the nearest integer. This procedure requires a metric, which in general may not be efficiently computable. A purely algebraic definition of noise is elements sampled from a secret normal subgroup $N \leq H$ because these can be efficiently erased by projecting onto the quotient H/N. In this setting, noise does not accumulate, meaning unbounded depth homomorphic operations can be performed without the need for inefficient bootstrapping.

The primary motivations behind considering learning with noise problems outside of the LWE setting are to avoid bootstrapping, which is necessary to deal with noise accumulation, and to avoid the best attacks on LWE-based encryption, as they are instance-specific for $\mathbb{F}_q$. The primary difficulties of the generic group learning with noise problems are the quantum and classical attacks presented in [1] (see Section 3.1) on finite abelian instances as well as finding non-abelian, efficient instances where this problem is hard.

Motivation: The main motivation of this work was to find a concrete instance for the Leonardi and Ruiz-Lopez framework. Given the classical and quantum attacks on the abelian case, it was reasonable to look for non-abelian instances. While non-commutativity seems to better protect against attacks, it also limits cryptographic capabilities. One solution suggested in [14] is to embed the non-abelian group in a group ring. But we then need to modify Leonardi and Ruiz-Lopez encryption to sample noise from *ideals* of the group ring.

1.1 Our results

Our results address **finite** groups and group rings and include:

- Generalizing and formalizing the set-up and security assumptions for Li and Wang's application of Ostrovsky and Skeith's Transform in [14].
- Reducing the quantum security of Li and Wang's multiplicative and fully homomorphic encryption schemes.
- Attempting to generalize Li and Wang encryption so that its security does not rely on RSA primes.

– Proving that it is infeasible to instantiate Leonardi and Ruiz-Lopez encryption on group rings, and more generally any efficiently decomposable semisimple rings, eliminating a large class of non-commutative structures.

The layout of the paper is as follows: in section 2 we review the mathematical background. In section 3 we review the three cryptographic primitives that are combined for our construction: the generalized LWE problem proposed by Leonardi and Ruiz-Lopez in [12], the transform from a multiplicative scheme on a simple non-abelian group to a fully homomorphic scheme given by Ostrovsky and Skeith in [18], and the fully homomorphic scheme proposed by Li and Wang based on group rings on simple non-abelian groups in [14]. In section 4 we present our construction for a "noise non-accumulating" fully homomorphic cryptosystem: an Ostrosky-Skeith Transform on a modification of Li and Wang encryption inspired by the Leonardi and Ruiz-Lopez homomorphism learning problem. We discuss sampling secret keys efficiently and prove that the an instance based on group rings does not satisfy the security requirements in [1]. We also suggest areas of further research.

1.2 Other Non-Commutative FHE Schemes

Cheng et al. provide a generalization of LWE to group rings in [5]. A concrete example they study is the group ring $\mathbb{Z}[D_{2n}]$, where D_{2n} is the *dihedral group* of order $2n$, which is non-abelian. The main advantage of considering non-abelian groups in LWE is to avoid attacks on principal ideal lattices. Their proposed encryption scheme uses noise that is measured by the size of the coefficients of elements in the group ring; this scheme has the disadvantage of accumulating noise.

Li and Wang introduce a noise non-accumulating fully homomorphic framework, different from the one our construction is based on, also using analogous matrix conjugation techniques [13]. The framework uses a non-commutative ring because it is unclear how to recover a message, which according to the decryption algorithm is the solution to a multi-variable linear system of equations, when variables do not commute. It seems that non-commutativity also protects against eigenvalue attacks. While this framework does not rely on quantum-insecure RSA primes like in [14], it does fail to be IND-CPA in general.

An approach that is similar to ours in the use of the Ostrovsky and Skeith transform to construct a noise non-accumulating fully homomorphic scheme is by Nuida [16]. After proving that a naive approach using matrix rings is susceptible to "linear attacks", the author proposes instead basing a scheme on Coxeter groups from combinatorial group theory. However, the scheme as presented in [16] suffers from unbounded ciphertexts, meaning that only a bounded number of homomorphic operations can be performed despite the fact that noise does not accumulate.

In general, constructing a fully homomorphic secure scheme without bootstrapping is a difficult problem. See [24] for more weaknesses of multiple proposed schemes.

Acknowledgements We thank Nick Priebe for valuable discussions on representation theory.

2 Preliminaries

2.1 Groups

Let G be a set equipped with an associative binary operation $\cdot : G \times G \to G$. We call $e \in G$ an identity element if $e \cdot g = g \cdot e = g$ for every $g \in G$. The identity element is unique, if it exists. We call $(G, \cdot)$ a *monoid* if it contains the identity. Given a $g \in G$, we say that another element is the *inverse* of g in G, denoted g^{-1}, if $g \cdot g^{-1} = g^{-1} \cdot g = e$. The inverse of an element is unique, if it exists. We call a monoid $(G, \cdot)$ a *group* if it also contains an inverse element g^{-1} for each $g \in G$. A group is *abelian* (or *commutative*) if $g \cdot h = h \cdot g$ for any two elements $g, h \in G$. From now on, to denote the group operation we may write gh, or $g+h$ if the context is abelian, in place of $g \cdot h$. If G is a group, we say that H is a *subgroup* of G if H is a non-empty subset of G closed under the group operation and inverses, and denote this by $H \leq G$. The *center* of a group is the set $Z(G) := \{g \in G : gh = hg \text{ for all } h \in G\}$.

Given two groups G_1 and G_2, a mapping $\varphi : G_1 \to G_2$ is a *(group) homomorphism* if $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$. A bijective homomorphism is called an *isomorphism*. Two groups G_1 and G_2 are said to be *isomorphic* if there exists an isomorphism $\varphi : G_1 \to G_2$, and we write this as $G_1 \cong G_2$. The *kernel* of a homomorphism $\varphi : G_1 \to G_2$ is the set $ker(\varphi) := \{g \in G_1 : \varphi(g_1) = e_{G_2}\} \subseteq G_1$, where e_{G_2} is the identity in G_2. The *image* of φ is defined to be $Im(\varphi) := \{h \in G_2 : h = \varphi(g) \text{ for some } g \in G\}$. The kernel and image of a homomorphism are subgroups of G_1 and G_2, respectively. We say that $H \leq G$ is *normal* if it is the kernel of a group homomorphism with domain G, and denote this $H \trianglelefteq G$. We always have $\{e\}, Z(G), G \trianglelefteq G$, and any subgroup of an abelian group is normal. A group is called *simple* if it has no normal subgroups different from $\{e\}$ and itself. Given a normal subgroup $H \trianglelefteq G$, we can construct the *quotient group* G/H, which is the set of (left) cosets of H in G equipped with the well-defined group operation $gH \cdot hH = ghH$ for any $gH, hH \in G/H$. The *First Isomorphism Theorem* says that, for any homomorphism $\varphi : G_1 \to G_2$, $G/ker(\varphi) \cong Im(\varphi)$. The *Correspondence Theorem* says that, if $N \trianglelefteq G$, then there is a 1-1 correspondence between subgroups $N \leq H \leq G$ and subgroups $H/N \leq G/N$. The *Third Isomorphism Theorem* says that this correspondence is normality-preserving; that is, if we further have that $H \trianglelefteq G$, then $H/N \trianglelefteq G/N$ and $(G/N)/(H/N) \cong G/H$.

Permutation Groups For $n \in \mathbb{N}$, the set S_n is the set of all bijections $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$, which forms a group when equipped with the composition operation. Elements of S_n are called *permutations* and are written using *cyclic notation*, where $\sigma = (a_1\ a_2\ \ldots\ a_m)$ means $\sigma(a_i) = a_{i+1}$ for all $1 \leq i < m$

and $\sigma(a_m) = a_1$, and cycles that are written side by side are multiplied. A *transposition* is a permutation of the form $(a_1\ a_2)$ for some $a_1, a_2 \in \{1, \ldots, n\}$. We define the homomorphism $sgn : S_n \to S_n$ by $sgn(\sigma) = 1$ if $\sigma \in S_n$ can be written as the product of an even number of transpositions, in which case we call σ an even permutation, and $sgn(\sigma) = -1$ otherwise, in which case we call σ an *odd permutation*.

The set of all even permutations of S_n form a subgroup called A_n. It is a well-known fact that A_5 is the smallest non-abelian, simple group.

2.2 Group Rings and Group Algebras

A *ring* is a set R equipped with two operations, called addition and multiplication and denoted $+$ and $\times$, so that $(R, +)$ is an abelian group, $(R, \times)$ is a monoid, and left and right distributivity hold. The additive and multiplicative identities are denoted 0_R and 1_R, resp. A *ring homomorphism* is a map between two rings that respects the ring operations.

For a ring R, an *R-module* is a set A equipped with a scalar multiplication operation $\cdot : R \times A \to A$, so that $1_R \cdot a = a$ for all $a \in A$ and left and right distributivity hold. An R-module A is called *free* if there exists a subset $B \subseteq A$ so that every element of A is a unique, R-linear combination of elements in B. In this case we would call B a *basis*. Given a free R-module A with basis $B = \{b_1, \ldots, b_N\}$, we define a map $[\cdot]_{b_i} : A \to R$ which given $a \in A$, outputs the coefficient on b_i in the unique R-linear combination of the basis B that equals a. If the context is clear, we use the shorthand $a_i := [a]_{b_i}$.

An *R-algebra* is a ring S that is an R-module, such that left and right distributivity hold. An *R-algebra homomorphism* is a map between two R-algebras which respects the R-algebra operations.

A *field* is a ring K such that every non-zero element has a multiplicative inverse. Such elements are called *units*. A *vector space* is a K-module, where K is a field. Vector spaces are always free. The vector space K^N is the set of all linear combinations of $\{e_i : 1 \leq i \leq N\}$, where e_i is the N-tuple that contains 1 in the i-th entry and 0 everywhere else.

An *integral domain* is a ring R that does not contain any non-zero elements $a \in R$ for which there exist $b \in R$ with $ab = 0$; such elements are called *zero divisors*. In general, every unit is a non-zero divisor. If R is a finite ring, then every non-zero divisor is also a unit.

Given a group G and a ring R, the *group ring* $R[G]$ is the set of formal finite sums of elements in G with coefficients in R. Then $R[G]$, equipped with the natural addition, multiplication, and scalar multiplication operations, is an R-algebra. If both R and G are finite, then $|R[G]| = |R|^{|G|}$. See [19] for a thorough

introduction to group rings.

The group ring $K[G]$ is also a K-vector space with basis G. If $G = \{g_1, \ldots, g_N\}$, then $\nu : K[G] \to K^N$ is a K-vector space homomorphism given by linearly extending the map $g_i \mapsto e_i$. We always assume to order G so that $g_1 = e$ is the identity. We also have the *natural right-multiplication matrix ring embedding* $\rho : K[G] \hookrightarrow M_{N\times N}(K)$, given by

$$\rho(\alpha) = \rho\left(\sum_{i=1}^{N}[\alpha]_{g_i}g_i\right) := \left[[\alpha]_{g_j^{-1}g_i}\right]_{\substack{1\le i\le N\\ 1\le j\le N}}$$

where $[\alpha]_{g_i} \in K$ is the coefficient of $g_i \in G$ on α. Then ρ is an R-algebra homomorphism and for any $\alpha, \beta \in R[G]$,

$$[\beta \cdot \alpha]_{g_i} = [\rho(\alpha)\nu(\beta)]_{e_i}$$

Notice that $\nu(\alpha)$ is simply the first column of the matrix $\rho(\alpha)$.

Given a prime p, the integers modulo p form a field and are denoted $\mathbb{F}_p$. We are primarily interested in the group ring $\mathbb{F}_p[A_5]$.

An R-module is called *simple* if it is non-zero and has no non-zero proper R-submodules. A ring is called *semisimple* if it is the direct sum of simple modules over itself.

2.3 Ideals and Zero Sets

Given a ring R, we say that $I \subseteq R$ is a left (resp. right) *ideal* of R if $(I, +)$ is a subgroup of $(R, +)$ and $rI \subseteq I$ for all $r \in R$. Ideals are exactly the kernels of ring homomorphisms.

Given a K-algebra $A \subseteq M_{N\times N}(K)$, we say that $a \in A$ is a zero of a polynomial $f \in K[x_{11}, \ldots, x_{NN}]$ if $f(a) := f(a_{11}, \ldots, a_{NN}) = 0$. The *zero set of* f is $V_A(f) := \{a \in A : f(a) = 0\}$.The *ideal of a set of points* $S \subseteq A$ is $I(S) := \{f \in K[x_{11}, \ldots, x_{NN}] : f(a) = 0,\ \forall a \in S\}$.

We define the *coordinate ring on* A to be

$$\Gamma(A) := K[x_{11}, \ldots, x_{NN}]/I(A)$$

where $I(A) := \{f \in K[x_{11}, \ldots, x_{NN}] : f(a) = 0 \text{ for all } a \in A\}$ is the ideal of A, sometimes called the *defining equations* of A.

For the group ring $K[G]$, where $|G| = N$, we have $\Gamma(\rho(K[G])) \cong K[x_1, \ldots, x_N]$.

Determinental Zero Sets For any matrix $\left[m_{ij}\right]_{1\leq i,j\leq N} \in M_{N\times N}(K)$, we define its *determinant* to be

$$\begin{aligned} det\left(\left[m_{ij}\right]_{1\leq i,j\leq N}\right) &:= \sum_{\sigma\in S_N} sgn(\sigma) m_{1\sigma(1)}\dots m_{N\sigma(N)} \\ &= \sum_{\tau\in S_N} sgn(\tau) m_{\tau(1)1}\dots m_{\tau(N)N} \end{aligned}$$

We write *det* to also mean the polynomial

$$det\left(\begin{bmatrix} x_{11} & \dots & x_{1N} \\ \vdots & & \vdots \\ x_{N1} & \dots & x_{NN} \end{bmatrix}\right) \in K[x_{11},\dots,x_{NN}]$$

Given a K-algebra $A \subseteq M_{N\times N}(K)$, we have $V_A(det) = \{a \in A : det(a) = 0\}$ to be the *determinental zero set*. For the group ring $K[G]$, where $|G| = N$, we use the shorthand $V_{K[G]}(det) := V_{\rho(K[G])}(det)$. Further, if $\alpha \in K[G]$, then $det(\rho(\alpha)) = 0$ iff $\rho(\alpha)$ is non-invertible iff α is non-invertible so when $K[G]$ is finite, $V_{K[G]}(det)$ is exactly the set of zero divisors.

More generally, we may define a *determinental ideal of rank* r to be

$$I_r = \left(\left\{ det(M) : M \text{ is an } r\times r \text{ minor of } \begin{bmatrix} x_{11} & \dots & x_{1N} \\ \vdots & & \vdots \\ x_{N1} & \dots & x_{NN} \end{bmatrix} \right\}\right) \subseteq K[x_{11},\dots,x_{NN}]$$

Then the corresponding *zero set* is $V_{K[G]}(I_r) = \{\alpha \in K[G] : rank(\rho(\alpha)) < r\}$. Explicitely, $V_{K[G]}(det) = V_{K[G]}(I_N)$.

For a subgroup $H \leq G$, we define the *projection* of $\alpha \in R[G]$ to be $proj_H(\alpha) = \sum_{g\in H}[\alpha]_g g$. The proposition below gives a shortcut to computing the formula for the determinant polynomial for $K[G]$ by piecing together the determinant polynomials of $K[H]$ for subgroups $H \leq G$.

Proposition 1. *If $H \leq G$ and $x = \sum_{g\in G} x_g g$, where the x_g are distinct ambient variables for each $g \in G$, then $det(proj_H(x)) \mid det(x)$.*

Proof. Reorder G so that H is listed first. Since H is closed under the binary operation on G, we can block-decompose the matrix

$$\rho(x) = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$$

where $A = \rho(proj_H(x))$. Then by properties of the determinant,

$$det(proj_H(x)) = det(A) \mid det(A)det(D - CA^{-1}B) = det(x)$$

Augmentation Ideal For a group $K[G]$ and embedding $\rho : K[G] \hookrightarrow M_{N\times N}(K)$, we define the *determinant* and *trace* of an element $\alpha \in K[G]$ to be $det(\alpha) := det(\rho(\alpha))$ and $tr(\alpha) := tr(\rho(\alpha))$. By definition of the right-multiplication embedding, $tr(\alpha) = N \cdot [\alpha]_e$.

We are also interested in the *augmentation ideal*, which is defined as

$$\mathcal{I} := V_{K[G]}\left(\sum_{i=1}^{N}\sum_{j=1}^{N} x_{ij}\right) = \left\{\alpha \in K[G] : \sum_{i=1}^{N} \alpha_i = 0\right\}$$

for $N \nmid char(K)$. It is easy to verify that this set $\mathcal{I}$ indeed an ideal of $K[G]$: first, $0 \in \mathcal{I}$, and second, for all $\alpha, \beta \in \mathcal{I}$ and $\gamma \in K[G]$,

$$\sum_{i=1}^{N}(\alpha+\beta)_i = \sum_{i=1}^{N}\alpha_i + \sum_{i=1}^{N}\beta_i = 0 \implies \alpha+\beta \in \mathcal{I}$$

and

$$\sum_{i=1}^{N}(\gamma\alpha)_i = \sum_{i=1}^{N}(\alpha\gamma)_i = \sum_{i=1}^{N}\alpha_i \sum_{i=1}^{N}\gamma_i = \sum_{i=1}^{N}\gamma_i \sum_{i=1}^{N}\alpha_i = 0 \implies \alpha\gamma, \gamma\alpha \in \mathcal{I}$$

Proposition 2. *$\mathcal{I} \subseteq V_{K[G]}(det)$, where $G = \{g_1, \ldots, g_N\}$ is finite.*

Proof. Let $\alpha \in \mathcal{I}$. So $\sum_{i=1}^{N} \alpha_i = 0$. Then $\rho(\alpha) \cdot \nu\left(\sum_{i=1}^{N} kg_i\right) = \mathbf{0} \in K^N$ for any $k \in K$, so in particular $\rho(\alpha)$ is a zero divisor. Therefore $\rho(\alpha)$ is non-invertible, or equivalently, $det(\rho(\alpha)) = 0$.

Proposition 3. *$\mathcal{I}$ is an $N-1$ dimensional vector subspace of $K[G]$, where $G = \{g_1, \ldots, g_N\}$.*

Proof. Using the standard basis for $K[G]$, we may write

$$\mathcal{I} = \left\{\alpha \in K[G] : \sum_{i=1}^{N} \alpha_i = 0\right\} = span\left\{g_1 - g_i : i \neq 1\right\}$$

2.4 Lagrange Interpolation

The *Lagrange polynomial* $L(x)$ is the unique polynomial of lowest degree that fits a set of data. Specifically, given a data set $\{(a_i, b_i) : 1 \leq i \leq k\}$, where all the a_i are distinct, then $L(a_i) = b_i$ for each $1 \leq i \leq k$ and $deg(L(x)) \leq k-1$.

The construction is as follows: let $\{\ell_1(x), \ldots, \ell_k(x)\}$ be rational functions, each of degree $k-1$, defined by

$$\ell_i(x) = \prod_{\substack{1\leq j\leq k \\ j\neq i}} \frac{x - x_j}{x_i - x_j}$$

Then

$$L(x) = \sum_{i=1} b_i \ell_i(x)$$

One can check that $L(x)$ satisfies the required properties.

We use Lagrange interpolation for efficient determinant computations (see section 4.1). Specifically, we compute a bivariate function $L(x_1, x_2)$ using the data points $\{(a_i, b_i) : 1 \leq i \leq k\} = \{(a, L(x_1, a)) : a \in \mathbb{F}_p\}$, where p is greater than the x_2 degree of $L(x_1, x_2)$.

3 Existing Encryption Schemes

Next, we recall the three major works that we base our construction on: section 3.1 outlines the Leonardi and Ruiz-Lopez homomorphism learning problem and encryption, section 3.2 reviews Ostrovsky and Skeith's transformation from a multiplicative homomorphic scheme on a simple, non-abelian group to a fully homomorphic scheme, and section 3.3 describes Li and Wang's application of the transform.

Notation: We use lower-case and upper-case letters to denote messages and encryptions, resp.

3.1 Leonardi and Ruiz-Lopez Encryption

In this section, we describe an unbounded homomorphic symmetric encryption scheme proposed by Leonardi and Ruiz-Lopez [12, section 5.1]. We will refer to this as *LRL-encryption*.

Fix three public finite groups G, H, and K in which binary operations and element sampling can be performed efficiently; see [12] for a generalization to finitely generated groups.

$KeyGen(1^\lambda)$: given the security parameter λ and public, efficiently computable groups G, H, K, generate efficiently computable homomorphisms $\varphi : G \to H$ and $\psi : H \to K$. Compute $ker(\psi)$ and sample an element $\tau \in H \backslash ker(\psi)$. The secret key is $sk = (\varphi, \psi, \tau)$.

$Enc(sk, b)$: given the secret key $sk = (\varphi, \psi, \tau)$, the encryption of a bit $b \in \{0, 1\}$ is $Enc(\beta) = (g, \varphi(g)h\tau^b)$, for randomly chosen $g \in G,\ h \in ker(\psi)$.

$Dec(sk, C)$: given the secret key $sk = (\varphi, \psi, \tau)$ and an encryption $C = (g, h') \in G \times H$, compute $m = \psi(\varphi(g))^{-1} \cdot \psi(h')$. The decryption of (g, h') is a bit

$$Dec(sk, C) = \begin{cases} 0 & \text{if } m = 1_K \\ 1 & \text{if } m \neq 1_K \end{cases}$$

Security of LRL The security of LRL-encryption depends on the hanrdness of the *learning homomorphism with noise* (LHN) problem for the public groups G, H, K.

Definition 1 (LHN, Definition 2 in [12]). *We say that an algorithm $\mathcal{A}$ solves LHN for G, H, K if, for any $\varphi : G \to H$, $\mathcal{A}$ is able to learn φ with non-negligible probability, given a set of samples $(g, \varphi(g)h) \in G \times H$, where $g \in G$ and $h \in H$ are sampled uniformly.*

See [1] for more details about the necessary security properties for an instance of LRL-encryption. Here is a summary for symmetric encryption:

1. There are an exponential number of choices of homomorphisms $\varphi : G \to H$ and $\psi : H \to K$ such that $Z(H) \not\subseteq ker(\psi)$.
2. The number of normal subgroups in H is exponential in the security parameter.

We refer the reader to [1] for details on the known classical attacks on asymmetric LRL-encryption.When H is abelian, the security of LRL-encryption reduces to replacing G with its abelianization $G/[G, G]$, which is potentially a smaller group. See **Lemma 3** in [1].

Note that the remaining classical and quantum attacks on abelian LRL-encryption in [1] and [12] only apply to the asymmetric scheme. However, the existence of such attacks motivate the search for a non-abelian instance of LRL-encryption.

3.2 Ostrovsky and Skeith's Transform

Given any multiplicative homomorphic scheme over any non-abelian simple group, such as the group of alternating permutations on five elements A_5, Ostrovsky and Skeith construct a fully homomorphic scheme that encrypts bit-wise and whose security only relies on the security on the original multiplicative homomorphic scheme. We refer to this process as the *OS-transform* and review the key elements of the transform below.

Theorem 1. *(Theorem 2.1 of [18]). Given a finite, non-abelian, simple group G, any function $f : \{0,1\}^m \to \{0,1\}^n$ can be represented solely in terms of the group operation on G.*

Proof sketch: Cauchy's Theorem guarantees the existence of an element $x \in G$ of order 2. Then the commutator subgroup $[C_G(x), C_G(x)]$ is equal to the whole group G, where $C_G(x) := \{gxg^{-1} : g \in G\}$ denotes the *conjugacy class of x*. Therefore, there must exist a sequence of commutators $s_1, \ldots, s_r \in [C_G(x), C_G(x)]$ such that $x = s_1 \cdots s_r$. This gives two sequences of elements in

G, $\{g_i\}_{i=1}^r$ and $\{h_i\}_{i=1}^r$, such that $s_i = [g_i x g_i^{-1}, h_i x h_i^{-1}]$, and we can define the operator NAND:$\{e,x\}^2 \to \{e,x\}$ by

$$\text{NAND}(a,b) = x \prod_{i=1}^{r} [g_i a g_i^{-1}, h_i b h_i^{-1}]$$

One can check that this is the desired function. By associating $\{e,x\}$ with $\{0,1\}$, it is thus possible to represent any function $f : \{0,1\}^m \to \{0,1\}^n$ using the group operation in G, since NAND is a universal gate.

Corollary 1. *(Corollary 2.4 of [18]). Constructing a fully homomorphic scheme over a ring with identity is equivalent to constructing a group homomorphic encryption over any finite non-abelian simple group.*

See the full version [17] or [20] for more details.

Explicitly: Choose the elements $e = ()$, $x = (12)(34)$, $s_1 = (15342)$, $s_2 = (345)$, $g_1 = (354)$, $h_1 = (243)$, and $h_2 = ()$ as in [14]. So x is an order 2 permutation with $x = (s_1^4 s_2^2)^2 s_1^2$ and $s_i = [g_i x g_i^{-1}, h_i x h_i^{-1}]$ for $i \in \{1,2\}$. Under the OS-transform, the operator NAND:$\{e,x\}^2 \to \{e,x\}$ is given by $\text{NAND}(a,b) = x(s_1'^4 s_2'^2)^2 s_1'^2$, where $s_i' = [g_i a g_i^{-1}, h_i b h_i^{-1}]$ for $i \in \{1,2\}$.

Now suppose there is a symmetric, multiplicatively homomorphic encryption scheme

$$\mathcal{E}_M = (KeyGen_M, Enc_M, Dec_M, Mul_M)$$

where $KeyGen_M(\lambda)$ outputs a secret key sk under the security parameter λ, $Enc_M(sk,\cdot) : \mathcal{M} \to \mathcal{C}$ and $Dec_M(sk,\cdot) : \mathcal{C} \to \mathcal{M}$ are the encryption and decryption functions, and $\mathcal{M}$ and $\mathcal{C}$ are the message space and cipher space, respectively. The message space $\mathcal{M}$ comes equipped with an associative multiplication operation. The scheme $\mathcal{E}_M$ satisfies *soundness* if $Dec_M(sk, Enc_M(sk,m)) = m$ for all $m \in \mathcal{M}$ for any secret key. Also, $Mul_M : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ is an operation satisfying the compact ciphertext requirement (see [8]) supported by the encryption scheme; that is, $Dec_M(sk, Mul_M(Enc_M(sk,m_1), Enc_M(sk,m_2))) = m_1 \cdot m_2$ for any $m_1, m_2 \in \mathcal{M}$. For shorthand notation, we write $C_1 C_2$ to mean $Mul_M(C_1, C_2)$ when it is clear that C_1 and C_2 are ciphertexts. We also note that Mul_M only needs to output an encryption of the product of decryptions of two ciphertexts, *so it need not be deterministic.*

Suppose further that $A_5 \leq \mathcal{M}$. Then the OS-transform outputs a new, symmetric, fully homomorphic encryption scheme we denote

$$\mathcal{E}_F = (KeyGen_F, Enc_F, Dec_F, NAND_F)$$

as follows. First, $KeyGen_F$ outputs the secret key $sk = KeyGen_M(\lambda)$ and the public parameters $X = Enc(sk,x)$, $G_i = Enc_M(sk,g_i)$ and $H_i = Enc_M(sk,h_i)$ for $i \in \{1,2\}$. Let $\mu : \{0,1\} \to \{e,x\}$ map $0 \mapsto e$ and $1 \mapsto x$. Then Enc_F :

$\{0,1\} \to \mathcal{C}$ is defined by $Enc_F(sk, b) = Enc_M(sk, \mu(b))$ and $Dec_F : \mathcal{C} \to \{0,1\}$ is defined by $Dec_F(sk, C) = \mu^{-1}(Dec_M(sk, C))$. Soundness of $\mathcal{E}_F$ clearly follows from soundness of $\mathcal{E}_M$, and semantic security of $\mathcal{E}_F$ follows from semantic security of $\mathcal{E}_M$ (indistinguishability given an adversary with access to an encryption oracle).

Finally, $NAND_F : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ is defined by $NAND_F(C_1, C_2) = X(S_1^4 S_2^2)^2 S_1^2$, where

$$S_i = [G_i C_1 G_i^{-1}, H_i C_2 H_i^{-1}]$$

for $i \in \{1,2\}$. We note that $NAND_F$ outputs an encryption of the nand of the decryptions of two ciphertexts, so just like Mul_M it need not be deterministic.

Remark 1. The ciphertext space $\mathcal{C}$ equipped with Mul_M is not necessarily associative or commutative, even if $\mathcal{M}$ is, and $\mathcal{C}$ does not necessarily contain an identity or inverses, even if $\mathcal{M}$ does. However, the image of $\mathcal{C}$ under the projection Dec_M is $\mathcal{M}$, which we can require to be a group. So following *Remark 1* in [14], since the operation $NAND_F$ only requires taking inverses of encryptions of e, x, g_i, h_i for $i \in \{1,2\}$, then for $m \in \{e, x\}$ we stipulate that $Enc(sk, m)^{-1} := Enc(sk, m)$, and for $m \in \{g_1, g_2, h_1, h_2\}$, we stipulate that $Enc(sk, m)^{-1} := Mul_M(Enc(sk, m), Enc(sk, m))$. Then decryption on the output of $NAND_F$ is sound.

3.3 Li and Wang Encryption

In this section, we describe a noiseless encryption scheme by Li and Wang [14]. The scheme is built by applying the OS-transform [18] to a symmetric multiplicative homomorphic encryption scheme. We refer to it as *LW-encryption*. Here we show that the LW-encryption is insecure in a post-quantum setting.

In work published the same year [16, §5.2] it was explained that matrix conjugation does not add any additional security to a group-based FHE schemes (and they credit an anonymous reviewer). Their overview is that upper triangular matrices (which will be seen in 3.3) are distinguishable from generic matrices by a linear condition which can be easily tested, and matrix conjugation simply transforms this to a more complicated looking linear condition. This does not seem to immediately apply to the LW-encryption scheme as it is only a group-based HE scheme. This work [16] differs from our work where we show that a quantum adversary can recover partial secret information of the LW-encryption HE scheme, and also create a distinguisher when the underlying group is abelian.

In order to apply the OS-transform, A_5 (or, equivalently, any other non-abelian simple group) needs to embed into the message space of a multiplicative homomorphic scheme. But the non-abelian group operation is inconvenient to use for a cryptographic construction. In LW-encryption, A_5 is embedded into

the group ring $\mathbb{Z}_n[A_5]$, where n is a big Blum integer, via the natural inclusion map $\nu : G \hookrightarrow \mathbb{Z}_n[A_5]$. The unembedding map $\nu^{-1} : \mathbb{Z}_n[A_5] \to G$ is given by

$$\nu^{-1}(\alpha) = \begin{cases} g_i & \text{if } \alpha_i \neq 0 \text{ and } \alpha_j = 0,\ \forall j \neq i \\ \perp & \text{otherwise} \end{cases}$$

Symmetric Multiplicative Homomorphic Scheme $KeyGen_M(1^\lambda)$: Choose four sufficiently large primes p, p_0, q, q_0 such that $p = 2p_0 + 1 \equiv 3 \pmod 4$ and $q = 2q_0 + 1 \equiv 3 \pmod 4$ and define the Blum integer $n = pq$. Sample a random invertible matrix $H \in M_{2\times 2}(\mathbb{Z}_n[A_5])$. Output the secret key $sk = (H, p, q)$ and the public parameter n.

$Enc_M(sk, m)$: Sample random $\alpha, \beta, \gamma \in \mathbb{Z}_n[A_5]$ and $t \in \mathbb{Z}_n^*$. The encryption of $m \in A_5$ is

$$Enc(sk, m) = H \begin{bmatrix} pt \cdot \nu(m) + q\alpha & \beta \\ 0 & \gamma \end{bmatrix} H^{-1} \in M_{2\times 2}(\mathbb{Z}_n[A_5])$$

$Dec_M(sk, C)$: Compute the matrix $W = H^{-1}CH$. Then $m = \nu^{-1}(p \cdot W_{11})$, where W_{11} is the left-top corner entry of W.

$Mul_M(C_1, C_2)$: Output $C_1 \cdot C_2$.

See [14, section 2.2.2] for the proofs of soundness for $Dec_M(sk, C)$ and $Mul_M(C_1, C_2)$, i.e. for all $m \in A_5$,

$$m = Dec(sk, Enc(sk, m))$$

and

$$Dec_M(sk, Mul_M(C_1, C_2)) = Dec_M(sk, C_1) \cdot Dec_M(sk, C_2)$$

Symmetric Fully Homomorphic Scheme LW-encryption follows by applying the OS-transform (see section 3.2) to the specific scheme described in section 3.3 to obtain the symmetric, fully-homomorphic encryption

$$\mathcal{E}_F = (KeyGen_F, Enc_F, Dec_F, NAND_F).$$

Post-Quantum Security The security of LW-encryption relies on two secret primes p, q that factor the public parameter n. Shor's Algorithm allows an adversary with access to a quantum computer to recover these two primes [22].

Following the analysis in [23], we reduce the post-quantum security of the MHE scheme, and hence the FHE scheme, as they are presented in [14], if A_5 were replaced with an abelian group G. Let $n = pq$ be a big Blum integer, and suppose the adversary has access to a factoring oracle (such as a quantum computer) so she knows p and q.

Lemma 1. *Each matrix A with invertible diagonal entries is of the form*

$$\mathcal{D}\begin{bmatrix}1 & b\\ c & 1\end{bmatrix}$$

where $\mathcal{D}$ is a diagonal matrix.

Proof. Write

$$A=\begin{bmatrix}h_1 & h_2\\ h_3 & h_4\end{bmatrix} \implies A=\begin{bmatrix}h_1 & 0\\ 0 & h_4\end{bmatrix}\begin{bmatrix}1 & h_2/h_1\\ h_3/h_4 & 1\end{bmatrix}$$

The MHE in section 3.3 uses a secret matrix $H \in M_{2\times 2}(\mathbb{Z}_n[G])$ as a private key and encrypts $m \in G$ by

$$Enc(H,m)=H\begin{bmatrix}pt\cdot\nu(m)+q\alpha_0 & \beta\\ 0 & \gamma\end{bmatrix}H^{-1}\in M_{2\times 2}(\mathbb{Z}_n[G])$$

Writing H^{-1} as in Lemma 1, since the diagonal entries are invertible with overwhelming probability, and using that diagonal matrices commute in the abelian setting, we see that $Enc(H,m)$ equals

$$\begin{bmatrix}1 & b\\ c & 1\end{bmatrix}^{-1}\mathcal{D}^{-1}\begin{bmatrix}pt\cdot\nu(m)+q\alpha & \beta\\ 0 & \gamma\end{bmatrix}\mathcal{D}\begin{bmatrix}1 & b\\ c & 1\end{bmatrix}=\begin{bmatrix}1 & b\\ c & 1\end{bmatrix}^{-1}\begin{bmatrix}pt\cdot\nu(m)+q\alpha & \beta\\ 0 & \gamma\end{bmatrix}\begin{bmatrix}1 & b\\ c & 1\end{bmatrix}$$

It is sufficient for an adversary to recover $b, c \in \mathbb{Z}_n[G]$. If $Enc(H,m)=\begin{bmatrix}A & B\\ C & D\end{bmatrix}$, then

$$\begin{aligned}\begin{bmatrix}1 & b\\ c & 1\end{bmatrix}\begin{bmatrix}A & B\\ C & D\end{bmatrix}=\begin{bmatrix}A+bC & B+bD\\ cA+C & cB+D\end{bmatrix}&=\begin{bmatrix}pt\cdot\nu(m)+q\alpha & \beta\\ 0 & \gamma\end{bmatrix}\begin{bmatrix}1 & b\\ c & 1\end{bmatrix}\\ &=\begin{bmatrix}pt\cdot\nu(m)+q\alpha+\beta c & pt\cdot\nu(m)b+q\alpha b+\beta\\ \gamma c & \gamma\end{bmatrix}\end{aligned}$$

Therefore, $\gamma = cB + D$ and $\gamma c = cA + C \implies c^2B + c(D - A) - C = 0$. As we are in the abelian setting, we can then recover c using the quadratic formula, assuming that B is invertible:

$$c=\frac{-(D-A)\pm\sqrt{(D-A)^2+4BC}}{2B}$$

To solve the square root in $\mathbb{Z}_n[G]$, project onto $\mathbb{F}_p$ and $\mathbb{F}_q$ and combine solutions using the Chinese Remainder Theorem. If given $Y \in K[G]$, for K a field, to solve the equation $X^2 = Y$ it suffices to solve $\rho(X)^2 = \rho(Y)$, since ρ is injective.

Distinguishing encryptions from random noise. Let

$$\mathcal{C}=\begin{bmatrix}A & B\\ C & D\end{bmatrix}\in M_{2\times 2}(K[G])$$

First, WLOG assume the coefficients on B are uniformly distributed whenever $\mathcal{C}$ is a valid encryption; otherwise, encryptions would be distinguishable. Construct the one variable polynomial $F(x_1) = det(x_1 \cdot e + \sum_{i=2}^{N} B_i g_i) \in K[x_1]$. Then B is non-invertible iff $det(B) = F(B_1) = 0$. Since the first coefficient $B_1 \in K$ is uniformly distributed and the N degree polynomial $F(x_1)$ has at most N roots, for $|K| \gg N$ the probability that B is invertible is close to 1 (essentially, the space of non-invertible matrices has codimension 1).

In that case, if $\mathcal{C}$ is a valid encryption of $m \in A_5$, then $Y := (D-A)^2 + 4BC$ is a perfect square in $K[G]$. By the same arguments as above, we can also assume that the coefficients of Y are uniformly distributed and Y is invertible, i.e. $\rho(Y)$ has full rank, with high probability; otherwise, encryptions would be distinguishable by computing this Y. Recall the ideal of $\rho(K[G])$ is $I(\rho(K[G]) = (x_{22} - x_{11}, x_{21} - x_{12}, \ldots, x_{NN} - x_{11})$, which is prime because $\Gamma(\rho(K[G])) \cong K[x_1, \ldots, x_N]$ is an integral domain. Hence, $\rho(K[G])$ is a variety.

The set of matrices in $\rho(K[G])$ that have repeated eigenvalues are exactly the vanishing place of the polynomial that maps a matrix representation of a group ring element to the discriminant of its characteristic polynomial $\rho(Y) \mapsto \prod_{i \neq j}(\lambda_i - \lambda_j)$. From algebraic geometry, either this set has codimension 1, or every matrix in $\rho(K[G])$ has a repeated eigenvalue.

So by similar reasoning as above, when $|K| \gg N$ we can, with high probability, expect WLOG $\rho(Y)$ to have distinct eigenvalues. Then it is easy to characterize the square roots of $\rho(Y)$, if they exist. Working over a prime field, write the diagonalization as $\rho(Y) = P^{-1} diag(\lambda_1, \ldots, \lambda_N) P$, where $\lambda_1, \ldots, \lambda_N \in K$ are the eigenvalues of $\rho(Y)$ and $P \in M_{N \times N}(K)$ is invertible. Then $M^2 = \rho(Y)$ iff $M = P^{-1} diag(\sqrt{\lambda_1}, \ldots, \sqrt{\lambda_N}) P$, where any square root of each λ_i can be chosen, for each $1 \leq i \leq N$. Over a prime field $\mathbb{F}_p$, for all non-zero eigenvalues there are two choices of the square root $\sqrt{\lambda_i} = \pm \lambda_i^{\frac{p+1}{4}}$, yielding at most 2^N solutions M.

The probability that a randomly chosen element of $\mathbb{F}_p$ is a perfect square is $O(1/2)$. So given a diagonalization of $\rho(Y)$ with N distinct eigenvalues, the probability of all the eigenvalues having a square root in $\mathbb{F}_p$ is $O(1/2^N)$ in $\mathbb{F}_p$. Thus, the probability that a randomly chosen invertible $Y \in \mathbb{Z}_n[G]$ is a perfect square is $O(1/2^{2N})$. As this is an easily testable property, one can construct a distinguisher which guesses as a valid encryption if Y is a perfect square, and guesses as random noise otherwise. This distinguisher will be correct when given valid encryptions, and will only guess incorrectly on a random noise sample with probability of $O(1/2^{2N})$.

Remark 2. Since fully homomorphic LW-encryption builds on the multiplicative homomorphic scheme in 3.3, the above attack reduces its security as well.

Asymmetric LW-encryption: Further, Li and Wang propose a further modification to $\mathcal{E}_F$ as it is presented above to construct an asymmetric, fully homomorphic encryption ([14, section 2.2.4]). The security of the modification relies on the hardness of solving extended discrete logarithms in the ring of 2×2 matrices over the group ring $\mathbb{Z}_n[A_5]$. However, Myasnikov and Ushakov present a polynomial-time quantum algorithm to solve discrete logarithms for this setting [15].

Therefore, LW-encryption most likely does not belong in the realm of post-quantum cryptography.

4 Our Construction

Write $A_5 = \{e = \sigma_1, \sigma_2, \ldots, \sigma_N\}$ with $N = |A_5| = 60$.

Modifying LW-encryption from 3.3, we let $p \equiv 3 \pmod 4$ be a large public prime and take the message space to be $\mathcal{M} = \mathbb{F}_p[A_5]$. We have the usual inclusions $A_5 \hookrightarrow \mathbb{F}_p[A_5] \hookrightarrow M_{2\times 2}(\mathbb{F}_p[A_5])$.

Sample a secret ideal: let $\alpha_2, \ldots, \alpha_N \in \mathbb{F}_p$ be randomly chosen. Compute and factor

$$F(x_1) := det\left(\rho\left(x_1\sigma_1 + \sum_{i=2}^{N} \alpha_i\sigma_i\right)\right) \in \mathbb{F}_p[x_1]$$

Then let α_1 be any root of $F(x_1)$. Take the two-sided ideal

$$I := \langle\alpha\rangle := \left\langle \sum_{i=1}^{N} \alpha_i\sigma_i \right\rangle \subseteq V_{\mathbb{F}_p[A_5]}(det)$$

Remark 3. If α is a zero divisor in a finite group ring $K[G]$, then all the non-zero elements of the left and right ideals (and thus the two-sided ideal) generated by α are zero divisors.

See 4.1 for further details on sampling ideals and the relationship between the multiplicity of the chosen root α_1 and the size of the ideal $\langle\alpha\rangle$.

$KeyGen(1^\lambda)$: Let $I \subseteq \mathbb{F}_p[A_5]$ be a secret ideal sampled as above. Let $H \in M_{2\times 2}(\mathbb{F}_p[A_5])$ be a random invertible secret matrix. Output $sk = (I, H)$.

$Enc_M(sk, m)$: For $m \in A_5$, we encrypt similar to Section 3.3. Sample random $k \in \mathbb{F}_p^\times$, $h \in I$, and $\beta, \gamma \in \mathbb{F}_p[A_5]$. Let

$$Enc_M(sk, m) = H \begin{bmatrix} k\nu(m) + h & \beta \\ 0 & \gamma \end{bmatrix} H^{-1}$$

$Dec_M(sk, m)$: Given an encryption $C = Enc_M(sk, m)$, compute

$$M = H^{-1}CH$$

Then $Dec_M(sk, m) = \nu^{-1}(\overline{M_{11}})$, where $\overline{M_{11}}$ denotes the residue class in $\mathbb{F}_p[A_5]/I$ of the top left entry of M.

$Mul_M(C_1, C_2)$: Given $C_1 = Enc_M(sk, m_1)$ and $C_2 = Enc_M(sk, m_2)$,

$$Mul_M(C_1, C_2) = C_1C_2$$

Soundness of $Mul_M(C_1, C_2)$

$$Mul_M(C_1, C_2) = H \begin{bmatrix} k_1\nu(m_1) + h_1 & \beta \\ 0 & \gamma \end{bmatrix} \begin{bmatrix} k_2\nu(m_2) + h_2 & \alpha_3 \\ 0 & \alpha_4 \end{bmatrix} H^{-1}$$

The bottom left and top left entries of the product of the inner two matrices is, respectively, zero and

$$(k_1\nu(m_1) + h_1)(k_2\nu(m_2) + h_2) = k_1k_2\nu(m_1m_2) + h$$

where $h \in I$ is uniformly distributed. The bottom right and top right entries are also uniformly distributed.

Soundness of $Dec_M(sk, m)$ As described above, compute

$$M_{11} = (H^{-1}CH)_{11} = k\nu(m) + h.$$

Then $\nu^{-1}(\overline{M_{11}}) = \overline{m} \in \mathbb{F}_p[A_5]/I$. Decryption is sound if and only if $\overline{m} = \overline{m'} \implies m = m'$ for any $m, m' \in A_5$. See 4.2 for more details.

4.1 Secret Ideals

Experimental data shows that computing the determinant for a general matrix $\rho(\sum_{i=1}^{N} x_i g_i)$ is much less efficient than computing $det(\rho(\alpha))$ for any $\alpha \in K[G]$, because storing N-variable polynomial expressions in the matrix entries is too memory intensive. However, it is possible to compute parts of the general determinant. It is efficient to compute $det(\rho(\alpha(x_i))) \in K[x_i]$, where $\alpha(x_i) \in K[x_i][G]$ such that $(\alpha(x_i))_i = x_i$ and $(\alpha(x_i))_j \in K$ for all $j \neq i$. WLOG we may take $i = 1$; otherwise, perform finitely many elementary column operations to place all the variable entries in $\rho(\alpha(x_i))$ on the main diagonal (this amounts to choosing a different ordering for G). Then computing the determinant of an $N \times N$ matrix where all of the non-diagonal entries are in K is feasible.

Dimensions of Ideals Generated by Zero Divisors Fix $\alpha_2, \ldots, \alpha_N \in K$. Define $\alpha : K \to K[G]$ by $\alpha(x) = x\sigma_1 + \alpha_2\sigma_2 + \ldots + \alpha_N\sigma_N$. Also define $M : K \to \rho(K[G])$ by $M(x) = \rho(\alpha(x))$. Notice that given any $r \in K$,

$$M(x) = (x - r)I_N - (-M(r))$$

Let $y = x - r$. So $det(M(x)) = det(M(y + r))$ is the characteristic polynomial of $-M(r)$. That is, if $m \geq 0$ is the largest integer such that $(y-s)^m \mid det(M(y+r))$, then s is an eigenvalue of $-M(r)$ with algebraic multiplicity m.

In particular, if $\alpha(r)$ is a zero divisor, then $x - r = y \mid det(M(y + r)) = det(M(x))$. In that case, let $m_r \geq 1$ be the largest integer such that $(x - r)^{m_r} \mid det(M(x))$. That means that 0 is an eigenvalue of $-M(r)$ with algebraic multiplicity m_r.

By linear algebra, $-M(r) \sim \begin{bmatrix} 0 & B \\ 0 & D \end{bmatrix}$, where the top left block is of dimension $nullity(M(r)) \times nullity(M(r))$. So the characteristic polynomial $\rho_{-M(r)}(y)$ is

$$\rho_{-M(r)}(y) = y^{nullity(M(r))}\rho_D(y)$$

We see that $nullity(M(r)) \leq m_r$.

Note $nullity(M(r)) = dim(\{\alpha(r) \cdot \sigma_1, \ldots, \alpha(r) \cdot \sigma_N\}) = dim(\langle\alpha(r)\rangle)$.

Using Lagrange Interpolation Consider again the determinant of a general matrix $\det(\rho(\sum_{i=1}^{N} x_i g_i))$. Suppose we factor this determinant, in N variable $x_1, \ldots, x_N$, into the product of factors $\prod_{i=1}^{m} f_i(x_1, \ldots, x_N)^{e_i}$. Since roots of these factors correspond to zero divisors of $K[G]$, and hence principal ideals, a natural question to ask is if two distinct roots of a single factor give the same principal ideal. We will answer that question here in the negative.

Substituting the above function $M(x) = \rho(\alpha(x))$ for the general matrix will give a determinant with factors in one variable, say $\prod_{i=1}^{m} f_i(x)^{e_i}$. A linear factors of $\det(M(x))$ will correspond to a unique principal ideal, as they only have one root when K is a field, and so cannot be used to answer the question in the preceding paragraph. Further, the non-linear factors of $\det(M(x))$ correspond to no ideals at all, since if they had roots in K they would factor further. For these reasons, it is not sufficient to look at single variable expressions instead of the general matrix. However, a bivariate expression should be sufficient to find two roots of a single factor and answer our question.

Using similar notation, we may compute $\det(\rho(\alpha(x_1, j))) \in K[x_1]$ for each $1 \leq j \leq N$, where $\alpha(x_1, \cdot) : K \to K[G]$ is defined by $\alpha(x_1, x_2) = x_1\sigma_1 + x_2\sigma_2 +$

$\alpha_3\sigma_3 + \ldots + \alpha_N\sigma_N$. However, we found that the function $\det(\rho(\alpha(x_1, x_2)))$ is still too computationally intensive, even if substantially better than the generic case with N variables. Instead, using Lagrange Interpolation on the data $\{(j, \alpha(x_1, j)) : 1 \leq j \leq |K|\}$ as described in 2.4, one can recover the unique degree $|K|-1$ polynomial $\det(\alpha(x_1, x_2)) \in K[x_1, x_2]$. Note that this process can be iterated to recover $\det(\alpha(x_1, x_2, x_3))$, and so on, defined similarly. However, this algorithm is exponential in k and experimental data shows that it is infeasible beyond $\det(\alpha(x_1, x_2))$ for large p.

Now that we are able to feasibly compute two distinct roots of a single factor, say x_1, x_2 and x_1', x_2', we have empirical evidence that they need not generate the same (one- or two-) sided ideals. That is, $\langle \alpha(x_1,\ x_2) \rangle \neq \langle \alpha(x_1',\ x_2') \rangle$ in general, and further, these ideals can have different dimension. See Appendix A for an example.

4.2 Soundness of Quotient

Let $G = A_5$ and $K = \mathbb{F}_p$. In order for the choice of secret ideal I to yield a sound $Dec(sk, \cdot)$ algorithm, we must have the following injective homomorphism that is the identity on G:

$$\varphi : G \hookrightarrow K[G] \hookrightarrow K[G]/I \hookrightarrow G$$

The first step $G \hookrightarrow K[G]$ is the inclusion homomorphism. The last step is $K[G]/I \hookrightarrow G$, $g_i + I \mapsto g_i$ for each $g_i \in G$. The last step is well-defined and φ is injective iff for all $g_i \neq g_j \in G$,

$$g_i - g_j \notin I \tag{1}$$

By Maschke's Theorem (see 2), $K[G]$ is principal, so $I = \langle \alpha \rangle$ for some $\alpha \in K[G]$ with $det(\alpha) = 0$.

It may be difficult to satisfy condition (1) above. But if the goal is to create a FHE scheme, then it is sufficient to distinguish between encryptions of $e \in A_5$ and $x \in A_5$, as they are defined in 3.2. To that end, order A_5 so that $g_1 := e$ is the first element and $g_{60} := x$ is the last element.

Sample a secret ideal: Follow the procedure in 4.1 to obtain a factored polynomial expression in one variable $F(x_1) := det(\rho(\alpha(x_1))) \in K[x_1]$. There is at least one linear factor

$$(x_1 + \sum_{i=2}^{N} \alpha_i) \mid F(x_1)$$

corresponding to an element of the augmentation ideal. From numerical analyses, if $p \equiv 1 \pmod 6$, we expect $F(x_1)$ to have other linear terms as well because of Euler's Criterion. Let $r \in K$ be a root of $F(x_1)$. Then substitute x for r to get $\alpha(r) \in K[G]$. Let $b = (1, 0, \ldots, 0, -1)^T \in K^N$. Row-reduce to check that

$\rho(\alpha(r))v = b$ has no solutions $v \in K^N$. If a solution exists, then $e - x \in \langle \alpha(r) \rangle$, so choose new random $\alpha_2, \ldots, \alpha_{60} \in K$ and repeat the procedure again.

Otherwise, $I = \langle \alpha(r) \rangle$ yields a sound decryption algorithm.

4.3 Number of Ideals in a Group Ring

Recall the following fundamental results in representation theory:

Theorem 2 (Maschke's Theorem). *If K is a field and G is a group such that $char(K) \nmid N$, then $K[G]$ is semisimple.*

Theorem 3 (Artin-Wedderburn Theorem). *If R is a finite-dimensional semisimple K-algebra for a field K, then R is isomorphic to a product of finitely many n_i-by-n_i matrix rings $M_{n_i}(D_i)$, where each D_i is a finite-dimensional division algebra over K, and both the n_i and D_i are unique up to permutation.*

Corollary 2. *If K is a field and G is a group such that $char(K) \nmid N$, then $K[G]$ is isomorphic to a unique (up to permutation) product $\prod_{i=1}^{m} M_{n_i}(D_i)$, with each D_i a finite-dimensional division algebra over K.*

From representation theory, m is the number of irreducible representations of G and equals the number of conjugacy classes of G. Each n_i is the dimension of an irreducible representation. Additionally,

$$|G| = \sum_{i=1}^{m} n_i^2$$

The group A_5 has 5 conjugacy classes. The unique way (up to relabelling) to write $|A_n| = 60$ as a sum of five squares is given by $n_1 = 1$, $n_2 = 3$, $n_3 = 3$, $n_4 = 4$, $n_5 = 5$.

Note: For $1 \leq i \leq n$, let $\Phi_i : G \to M_{n_i \times n_i}(D_i)$ be the ith representation, corresponding to each dimension n_i. Then the ith character is defined as $\chi_i : G \to D_i$ by $\chi_i(g) = tr(\Phi_i(g))$ for each $g \in G$. Since every Φ_i is a homomorphism, $\Phi_i(e) = I_{n_i}$, so $\chi_i(e) = n_i$.

The Wedderburn-Artin decomposition of $\mathbb{F}_p[A_5]$ is given by the product of the codomains of the irreducible representations (irreps) of A_5. So

$$\mathbb{F}_p[A_5] = M_{1\times1}(D_1) \times M_{3\times3}(D_2) \times M_{3\times3}(D_3) \times M_{4\times4}(D_4) \times M_{5\times5}(D_5) \quad (2)$$

Since $\mathbb{F}_p[A_5]$ is finite, each D_i is also finite. By Wedderburn's Little Theorem, each D_i is actually a finite field extension of $\mathbb{F}_p$. By comparing the number of elements on both sides of equation 2, we see that $D_i = \mathbb{F}_p$ for each $1 \leq i \leq 5$. From [10], we have

Proposition 4. *Every two-sided ideal of $M_{n\times n}(R)$ has the form $M_{n\times n}(I)$ for some unique two-sided ideal $I \subseteq R$.*

Note: The only left (resp. right) ideals in a division ring D are (0) and D. This is because, if there is an ideal $I \subseteq D$ with $0 \neq u \in I$, then $u^{-1}u = uu^{-1} = 1 \in D$. An easy consequence is that $M_{n\times n}(D)$ has no non-trivial two-sided ideals.

Therefore, there is a 1-1 correspondence between ideals of $\mathbb{F}_p[A_5]$ and ideals of $\prod_{i=1}^{5} M_{n_i\times n_i}(\mathbb{F}_p)$, which are exactly of the form $\langle(b_1, b_2, b_3, b_4, b_5)\rangle$ with each $b_i \in \{0, 1\}$. So $\mathbb{F}_p[A_5]$ has $2^5 = 32$ two-sided ideals.

Remark 4. By Artin-Wedderburn decomposition of semisimple rings, if $char(K) \nmid N$, then $K[G]$ is a principal ideal domain. The decomposition of $\mathbb{F}_p[A_5]$ shows that there are 5 maximal two-sided ideals: these are generated by $(1, 1, 1, 1, 0)$, $(1, 1, 1, 0, 1)$, $(1, 1, 0, 1, 1)$, $(1, 0, 1, 1, 1)$, $(0, 1, 1, 1, 1)$, using the shorthand as above, and similarly 5 minimal ideals. In particular, $\mathbb{F}_p[A_5]$ is not a local ring. Also, in light of section 4.1, given an ideal $I = \langle(b_1, b_2, b_3, b_4, b_5)\rangle$, $dim(I) = b_1 + 9b_2 + 9b_3 + 16b_4 + 25b_5$.

The above results apply to all finite K-algebras $K[G]$. The number of two-sided ideals of $K[G]$ is constant with respect to the size of K, as long as $char(K) \nmid N$. Therefore, $K[G]$, as well as any finite semisimple ring whose decomposition can be efficiently computed, is an inadequate context for a (ring) homomorphism learning problem for non-commutative LRL-encryption.

One-Sided Ideals One may consider instead using left (resp. right) ideals, but two problems arise: first, both left and right noise accumulates in the product during the Mul_M operation described in 4:

$$(k_1m_1 + h_1)(k_2m_2 + h_2) = k_1k_2m_1m_2 + k_2h_1m_2 + k_1m_1h_2 + h_1h_2$$

so the encryption scheme as it is presented in 4 is not compatible with one-sided ideals as secret keys; second, and more generally, the following proposition shows that the number of one-sided ideals in $K[G]$ does not grow with the security parameter p.

Proposition 5. *Let $n \in \mathbb{N}$ and K be a field. Then the left (resp. right) ideals of $M_{n\times n}(K)$ are in bijection with the subspaces of K^n.*

Proof. Given a subspace $V \subseteq K^n$, define $I \subseteq M_{n\times n}(K)$ to be the set of matrices that vanish on V. One can show that I is a left ideal. Conversely, given a left ideal $I \subseteq M_{n\times n}(K)$, let

$$V = \bigcap_{x\in I} Null(x) \subseteq K^n$$

V is an intersection of subspaces so it is itself a subspace. One can show this gives a 1-1 correspondence between left ideals and subspaces. The argument is symmetrical for right ideals.

Remark 5. The above result generalizes to ideals of $M_{n\times n}(R)$ and R-submodules of R^n, where R is an associative, unital ring.

4.4 Future Work

Our work shows that group rings are incompatible with the current model for LRL-encryption. Given the existing abelian classical and quantum attacks, we plan to consider other non-abelian groups and rings for instantiating LRL-encryption and prove security results or construct attacks.

One interesting avenue is to consider finitely generated groups, and use general probability distributions instead of uniform sampling, as described in [12]. In particular, Coxeter groups seem to yield more fruitful results as in [16], and they are not as simply decomposed as semisimple rings.

Further work can also be done using isogeny cryptography; while [12] showed that instantiating LRL encryption with isogenies as the secret homomorphisms φ and ψ is not quantum secure, it would be interesting to consider the group elements of the public G, H, and K themselves to be isogenies, as the endomorphism rings of supersingular curves over (over an algebraically closed field of finite characteristic) are non-commutative.

References

1. Eleni Agathocleous, Vishnupriya Anupindi, Annette Bachmayr, Chloe Martindale, Rahinatou Yuh Njah Nchiwo, and Mima Stanojkovski. On homomorphic encryption using abelian groups: Classical security analysis, 2023.
2. Frederik Armknecht, Tommaso Gagliardoni, Stefan Katzenbeisser, and Andreas Peter. General impossibility of group homomorphic encryption in the quantum world, 2014.
3. Zvika Brakerski and Vinod Vaikuntanathan. Efficient fully homomorphic encryption from (standard) lwe. In *2011 IEEE 52nd Annual Symposium on Foundations of Computer Science*, pages 97–106, 2011.
4. Zvika Brakerski and Vinod Vaikuntanathan. Fully homomorphic encryption from ring-lwe and security for key dependent messages. In *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference*, volume 6841 of *Lecture Notes in Computer Science*, page 501. Springer, 2011.
5. Qi Cheng and Jincheng Zhuang. Lwe from non-commutative group rings. *Designs, Codes and Cryptography*, 90:239–263, 2016.
6. Jung Hee Cheon, Kyoohyung Han, Andrey Kim, Miran Kim, and Yongsoo Song. Bootstrapping for approximate homomorphic encryption. Cryptology ePrint Archive, Paper 2018/153, 2018. `https://eprint.iacr.org/2018/153`.
7. Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *Advances in Cryptology – ASIACRYPT 2016*, pages 3–33, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg.
8. Craig Gentry. *A fully homomorphic encryption scheme*. PhD thesis, Stanford University, 2009. `crypto.stanford.edu/craig`.
9. Craig Gentry, Shai Halevi, and Nigel P. Smart. Better bootstrapping in fully homomorphic encryption. Cryptology ePrint Archive, Paper 2011/680, 2011. `https://eprint.iacr.org/2011/680`.
10. Pierre Antoine Grillet. *Abstract Algebra*, chapter 9. Springer New York, 2009.

11. Wonkyung Jung, Sangpyo Kim, Jung Ho Ahn, Jung Hee Cheon, and Younho Lee. Over 100x faster bootstrapping in fully homomorphic encryption through memory-centric optimization with gpus. Cryptology ePrint Archive, Paper 2021/508, 2021. https://eprint.iacr.org/2021/508.
12. Christopher Leonardi and Luis Ruiz-Lopez. Homomorphism learning problems and its applications to public-key cryptography, 2019.
13. Jing Li and Licheng Wang. Noise-free symmetric fully homomorphic encryption based on non-commutative rings. Cryptology ePrint Archive, Paper 2015/641, 2015. https://eprint.iacr.org/2015/641.
14. Jing Li and Licheng Wang. Noiseless fully homomorphic encryption, 2017.
15. A. D. Myasnikov and A. Ushakov. Quantum algorithm for the discrete logarithm problem for matrices over finite group rings. Cryptology ePrint Archive, Paper 2012/574, 2012. https://eprint.iacr.org/2012/574.
16. Koji Nuida. Towards constructing fully homomorphic encryption without ciphertext noise from group theory. Cryptology ePrint Archive, Paper 2014/097, 2014. https://eprint.iacr.org/2014/097.
17. Rafail Ostrovsky and William E. Skeith III. Algebraic lower bounds for computing on encrypted data. Cryptology ePrint Archive, Paper 2007/064, 2007. https://eprint.iacr.org/2007/064.
18. Rafail Ostrovsky and William E. Skeith. Communication complexity in algebraic two-party protocols. In David Wagner, editor, *Advances in Cryptology – CRYPTO 2008*, pages 379–396, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg.
19. Donald S. Passman. *The Algebraic Structure of Group Rings*. A Wiley-Interscience publication. Wiley, 1977.
20. Doerte K. Rappe. Homomorphic cryptosystems and their applications. Cryptology ePrint Archive, Paper 2006/001, 2006. https://eprint.iacr.org/2006/001.
21. Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing*, STOC '05, page 84–93, New York, NY, USA, 2005. Association for Computing Machinery.
22. Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, oct 1997.
23. Boaz Tsaban and Noam Lifshitz. Cryptanalysis of the more symmetric key fully homomorphic encryption scheme. *Journal of Mathematical Cryptology*, 9(2):75–78, 2015.
24. Yongge Wang. Notes on two fully homomorphic encryption schemes without bootstrapping. Cryptology ePrint Archive, Paper 2015/519, 2015. https://eprint.iacr.org/2015/519.
25. Alexander Wood, Kayvan Najarian, and Delaram Kahrobaei. Homomorphic encryption for machine learning in medicine and bioinformatics. *ACM Comput. Surv.*, 53(4), aug 2020.

A Ideals from Bivariate Determinants

A.1 Example in A_4

Consider the group algebra $\mathbb{Z}_{13}[A_4]$ (the choice of 13 is motivated by $\#A_4 = 12$, and the need for sufficient points in the field to perform Lagrange interpolation). Let $\alpha : \mathbb{Z}_{13} \times \mathbb{Z}_{13} \to \mathbb{Z}_{13}[A_4]$ be

$$\begin{aligned}\alpha(x,\ y) = x\ id(A_4) + y\ (13)(24) + 8(12)(34) + 8(14)(23) + 10(243) \\ +\ 2(134) + 6(123) + 9(142) + 11(234) + 9(132) + 7(124) + 8(143)\end{aligned}$$

Then, using Lagrange interpolation, we can compute and factor the associated determinant:

$$\begin{aligned}\det(\rho(\alpha(x,\ y))) = (x + y + 9)(x + y)^2(x^3 + 12x^2y + 12xy^2 \\ +\ y^3 + 10x^2 + 10y^2 + 6xy + 12x + 5y)^3\end{aligned}$$

Consider the following three roots corresponding to the quadratic factor $(x_1 + x_2)^2$ for this determinant.

$$\begin{aligned}\alpha_1 &= 0\ id(A_4) + 0(13)(24) + 8(12)(34) + 8(14)(23) + 10(243) + 2(134) \\ &\quad +\ 6(123) + 9(142) + 11(234) + 9(132) + 7(124) + 8(143), \\ \alpha_2 &= 6\ id(A_4) + 7(13)(24) + 8(12)(34) + 8(14)(23) + 10(243) + 2(134) \\ &\quad +\ 6(123) + 9(142) + 11(234) + 9(132) + 7(124) + 8(143), \\ \alpha_3 &= 1\ id(A_4) + 12(13)(24) + 8(12)(34) + 8(14)(23) + 10(243) + 2(134) \\ &\quad +\ 6(123) + 9(142) + 11(234) + 9(132) + 7(124) + 8(143).\end{aligned}$$

These three elements of $\mathbb{Z}_{13}[A_4]$ are all zero divisors, arising from the same factor of $\det(\rho(\alpha(x,\ y)))$, so to verify our claim from 4.1 we examine the (one-sided) ideals they generate. First, $\langle\alpha_1\rangle_L$ and $\langle\alpha_2\rangle_L$ have dimension 7 (where $\langle\cdot\rangle_L$ denotes the left-principal ideal), but they are not equal. Next, $\langle\alpha_3\rangle_L$ has dimension 10, and is therefore distinct from both $\langle\alpha_1\rangle_L$ and $\langle\alpha_2\rangle_L$.

A.2 Example in A_5

Since $\#A_5 = 60$, we use the field $\mathbb{Z}_{61}$ to have sufficient data for Lagrange interpolation. We chose random coefficients and set $\alpha : \mathbb{Z}_{61} \times \mathbb{Z}_{61} \to \mathbb{Z}_{61}[A_5]$ as

$$\begin{aligned}
\alpha(x,\ y) = x\ id(A_5) + y\ &(1,2,3) + 18(1,3,2) + 22(1,4,5,3,2) + 46(1,5,4,3,2) \\
+\ &57(2,3,4) + 39(1,2)(3,4) + 17(1,3,4) + 7(1,4)(3,5) + 59(1,5,4) \\
+\ &13(2,4,3) + 41(1,2,4) + 17(1,3)(2,4) + (1,4,2,5,3) \\
+\ &37(1,5,4,2,3) + 32(2,5,4) + 46(1,2,5,4,3) + 6(1,3,2,5,4) \\
+\ &54(1,4)(2,3) + 10(1,5,3,2,4) + 32(3,4,5) + 20(1,2,3,4,5) \\
+\ &43(1,3,4,5,2) + 34(1,4,3,5,2) + 57(1,5,2) + 21(2,3)(4,5) \\
+\ &4(1,2)(4,5) + 19(1,3)(4,5) + 15(1,4,3) + 10(1,5,3) + 37(2,4,5) \\
+\ &2(1,2,4,5,3) + 46(1,3,2,4,5) + 22(1,4,3,2,5) + 41(1,5)(2,3) \\
+\ &35(2,5,3) + 43(1,2,5) + 58(1,3)(2,5) + 19(1,4,5,2,3) \\
+\ &35(1,5,2,4,3) + 44(3,5,4) + 57(1,2,3,5,4) + 31(1,3,5,4,2) \\
+\ &33(1,4,2) + 54(1,5,3,4,2) + 9(2,3,5) + 33(1,3,5) + 10(1,4,5) \\
+\ &29(1,5)(3,4) + 59(2,4)(3,5) + 59(1,3,5,2,4) + 51(1,4)(2,5) \\
+\ &30(1,5,2,3,4) + (2,5)(3,4) + 25(1,2,5,3,4) + 28(1,3,4,2,5) \\
+\ &60(1,4,2,3,5) + 53(1,5)(2,4)
\end{aligned}$$

Then, using Lagrange interpolation, we can compute and factor the associated determinant, $\det(\rho(\alpha(x_1,\ x_2)))$. This is to large to print, and would be too computationally intensive for previous methods to compute. However, one factor is

$$\begin{aligned}
(&x^5 + 60x^4y + 41x^4 + x^3y^2 + 34x^3y + 36x^3 + x^2y^3 + 10x^2y^2 \\
&+ 22x^2y + 59x^2 + 60xy^4 + 31xy^3 + 24xy^2 + 20xy + 60x \\
&+ y^5 + 44y^4 + 6y^3 + 48y^2 + 26y + 49)^5
\end{aligned}$$

which has, among others, the roots $(2, 27)$ and $(5, 1)$. The (left- or right-) ideals generated by $\alpha(2, 27)$ and $\alpha(5, 1)$ each have dimension 55 and are distinct.